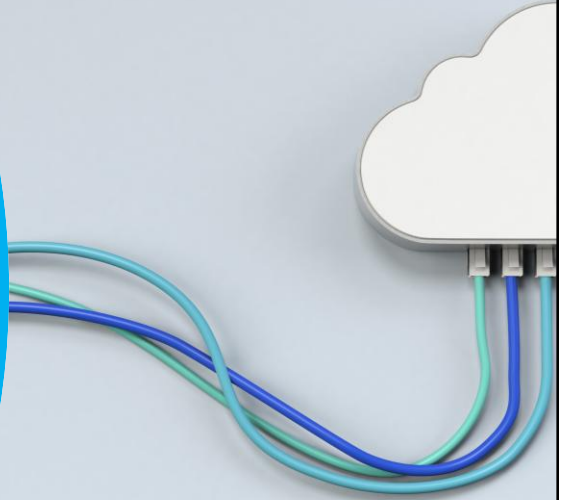


Klassifizierung von Netzwerken

NETZWERKTECHNIK / SEMESTER 1 UND 2



1

AGENDA

- 01 DARSTELLUNG UND TOPOLOGIEN
- 02 TYPEN VON NETZWERKEN
- 03 INTERNETVERBINDUNG
- 04 ZUVERLÄSSIGE NETZWERKE
- 05 SICHERHEIT
- 06

2

01

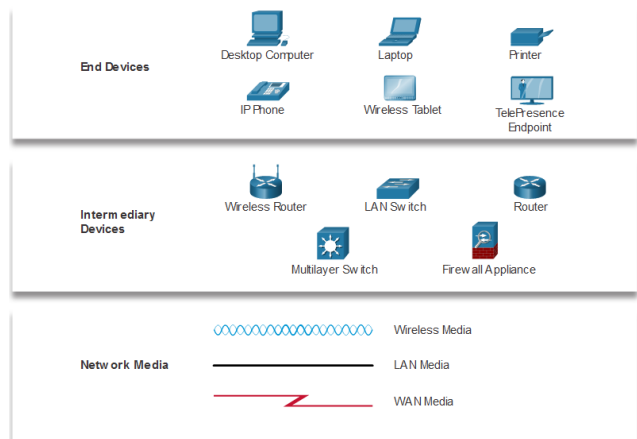
Darstellungen und Topologien

3

NETZWERKTECHNIK / SEMESTER 1 und 2

Network Representations

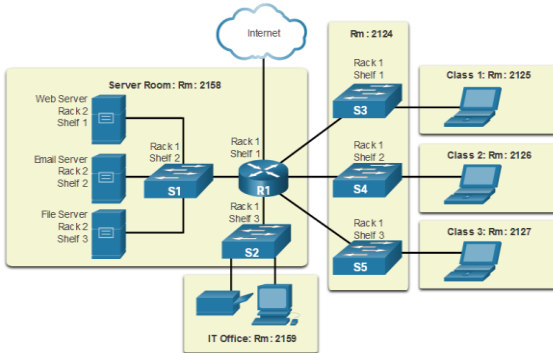
- Netzwerkdiagramme, die häufig als Topologie Diagramme bezeichnet werden, verwenden Symbole, um Geräte innerhalb des Netzwerks darzustellen.
- Wichtige Begriffe, die Sie kennen sollten, sind:
 - Netzwerkkarte (NIC)
 - Physischer Anschluss
 - Schnittstelle
- Logischen Darstellungen basierend auf den physischen Netzwerkkomponenten abzuleiten, ist entscheidend, um die Organisation und den Betrieb eines Netzwerks visualisieren zu können.
- Hinweis: Häufig werden die Begriffe Port und Schnittstelle als Synonym verwendet



4

Topologie Diagramme

- **Physikalische Topologie Diagramme** veranschaulichen die physische Position von Zwischengeräten und Kabelinstallationen.
- **Logische Topologie Diagramme** veranschaulichen Geräte, Ports und das Adressierungsschema des Netzwerks.



5

02

Typen von Netzwerken

6

Rechnernetzarten

- **Breitbandnetze** sind Zugänge zum Internet mit vergleichsweise hoher Datenübertragungsrates von einem Vielfachen der Geschwindigkeit älterer Zugangstechniken wie der Telefonmodem- oder ISDN-Einwahl, die zur Unterscheidung als Schmalbandtechniken bezeichnet werden
- **Mobilfunk- und Drahtlosnetze** sind drahtlose Netzwerke, die Hochfrequenzverbindungen (RF) zwischen den Knoten im Netzwerk nutzen
- **Netze für Content-Provider**, auch Content Delivery Network (CDN), sind Netzwerke aus geografisch verteilten Servern, mit dem Zweck Webinhalte schneller an Benutzer auszuliefern, indem es die Inhalte näher an den Standort der Benutzer cached.
- **Transitnetze** kommen zum Einsatz wenn der Content-Provider und Ihr Internetdienstanbieter (ISP, Internet Service Provider) nicht direkt miteinander verbunden sind. Dann sind sie häufig auf ein Transitnetz angewiesen, um den Verkehr zwischen ihnen zu übertragen. Transitnetze berechnen in der Regel sowohl dem Internetdienstanbieter als auch dem Content-Provider Gebühren für die Übertragung des Datenverkehrs von Ende zu Ende.
- **Unternehmensnetze** sind ein komplexes System miteinander verbundener Computer und Geräte innerhalb eines Unternehmens, das den Austausch von Daten und die Ausführung von Geschäftsprozessen ermöglicht

7

Netzwerke in vielen Größen

- **Kleine Heimnetzwerke** – verbinden Sie einige Computer miteinander und mit dem Internet
- **Small Office/Home Office** – ermöglicht die Verbindung von Computern zu Hause oder an entfernten Standorten mit einem Unternehmensnetzwerk
- **Mittlere bis große Netzwerke** – viele Standorte mit Hunderten oder Tausenden von miteinander verbundenen Computern
- **Weltweite Netzwerke** – verbindet Hunderte von Millionen von Computern weltweit – wie z.B. das Internet



Heimnetzwerke



SoHo



Mittlere bis Große

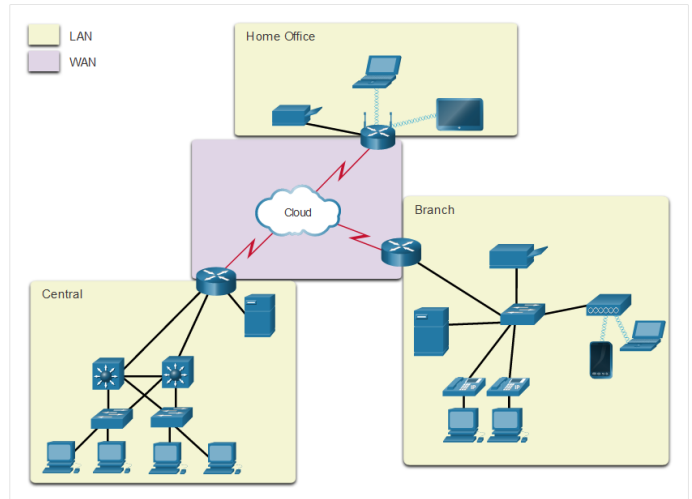


Weltweit

8

LAN und WAN

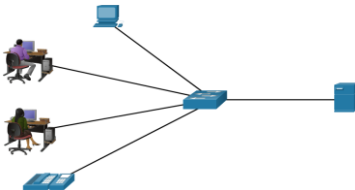
- Netzwerkinfrastrukturen unterscheiden sich stark in Bezug auf:
 - Größe des abgedeckten Bereichs
 - Anzahl der verbundenen Benutzer
 - Anzahl und Arten der verfügbaren Dienste
 - Aufgabenbereich
- Zwei gebräuchlichste Arten von Netzwerken:
 - Lokales Netzwerk (LAN)
 - Weitverkehrsnetz (WAN).



9

LAN und WAN

- **LAN** ist eine Netzwerkinfrastruktur, die sich über ein kleines geografisches Gebiet erstreckt.
- **Ein WAN** ist eine Netzwerkinfrastruktur, die sich über ein weites geografisches Gebiet erstreckt.

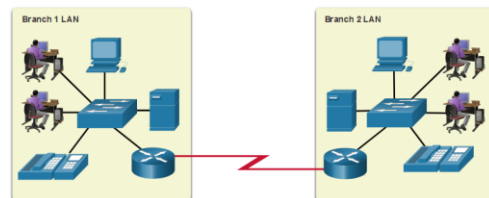


LAN

Endgeräte auf begrenztem Raum vernetzen.

Wird von einer einzelnen Organisation oder Einzelperson verwaltet.

Hohe Geschwindigkeiten für interne Endgeräte



WAN

Verbindet LANs über weite geografische Gebiete

Wird in der Regel von einem oder mehreren Dienst Anbietern verwaltet.

Langsamere Verbindungsgeschwindigkeiten zwischen LANs

10

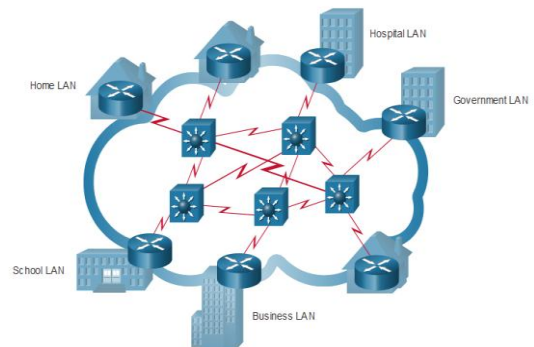
Einteilung der Netze nach ihrer Ausdehnung

Abkürzung	Bezeichnung	Beschreibung
LAN	Local Area Network	auf ein Betriebsgelände beschränktes Netz mit einer Ausdehnung von wenigen Kilometern, unter lokaler Administration
MAN	Metropolitan Area Network	auf eine Stadt beschränktes Netzwerk, häufig von Stadtwerken oder Kommunen betrieben
WAN	Wide Area Network	Weitverkehrsnetz, ein Netzwerk, das über den LAN-Bereich hinausgeht, öffentliche Netze von Anbietern wie Deutsche Telekom, Arcor usw. und unter Administration von diesen Anbietern
GAN	Global Area Network	Weltweites Netz, erdumfassend, z. B. Telefonnetz, Internet, ...
PAN	Private Area Network	Netzwerk im Privatbereich, Beschränkung auf wenige Meter, z. B. Bluetooth
CAN	Controller Area Network	Netzwerk von Mikrocontrollern, verbindet z. B. Steuergeräte in Kraftfahrzeugen

11

Das Internet

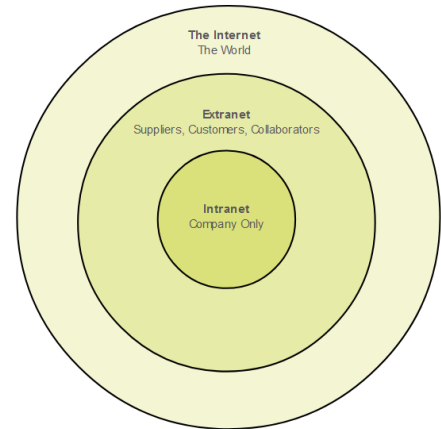
- Das Internet ist eine weltweite Ansammlung von miteinander verbundenen LANs und WANs.
- LANs werden über WANs miteinander verbunden
- WANs sind miteinander verbunden
- WANs können Kupferdrähte, Glasfaserkabel und drahtlose Übertragungen verwenden.
- Das Internet ist nicht Eigentum einer Einzelperson oder Gruppe. Die folgenden Gruppen wurden entwickelt, um die Struktur im Internet zu erhalten:
 - IETF
 - ICANN
 - IAB



12

Intranet und Extranet

- Ein **Intranet** ist eine private Sammlung von LANs und WANs, die innerhalb einer Organisation vorhanden sind und nur für die Mitglieder der Organisation oder andere Personen mit Berechtigung zugänglich sein sollen.
- Eine Organisation kann ein **Extranet** nutzen, um Personen, die für eine andere Organisation arbeiten und Zugriff auf Daten im Netzwerk benötigen, einen sicheren Zugriff zu gewähren.
 - Ein Unternehmen, das Zugang für externe Lieferanten und Auftragnehmern bietet
 - Ein Krankenhaus, das Ärzten ein Buchungssystem bereitstellt, damit Termine von Patienten verwalten werden können



03

Internet-verbinding

Internet Zugangstechnologien

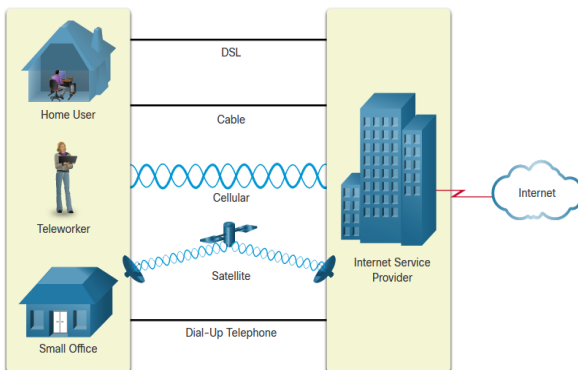
Es gibt viele Möglichkeiten, Benutzer und Organisationen mit dem Internet zu verbinden

- Zu den beliebten Diensten für Privatanwender und kleine Büros gehören Breitbandkabel, Breitband-DSL (Digital Subscriber Line), drahtlose WANs und mobile Dienste.
- Unternehmen benötigen schnellere Verbindungen, um IP-Telefone, Videokonferenzen und Speicher im Rechenzentrum zu unterstützen.
- Verbindungen der Business-Klasse werden in der Regel von Service Providern (SP) bereitgestellt und können Folgendes umfassen: Business-DSL, Standleitungen und Metro-Ethernet.



15

Heimnetzwerk und SoHo Internetverbindungen



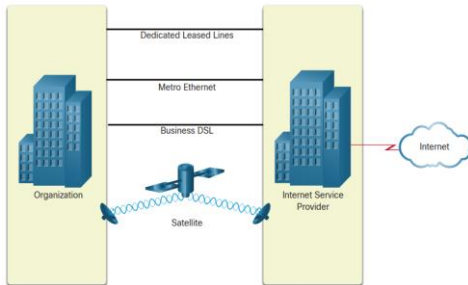
Verbindung	Beschreibung
Cable	Hohe Bandbreite, immer verfügbares Internet, das häufig von Kabelfernseh-anbietern angeboten wird.
DSL	Hohe Bandbreite, immer aktiv, Internetverbindung, die über eine Telefonleitung läuft.
Mobilfunk	Verwendet ein Mobilfunknetz, um eine Verbindung zum Internet herzustellen.
Satellit	großer Nutzen für ländliche Gebiete ohne Internet Service Provider.
FTTH (PON, AON)	Glasfaserkabel und Signale ganz oder größtenteils bis zum Endbenutzer

16

Business Internetverbindungen

▪ Geschäftsverbindungen von Unternehmen können Folgendes erfordern:

- Höhere Bandbreite
- Dedizierte Verbindungen
- Verwaltete Dienstleistungen

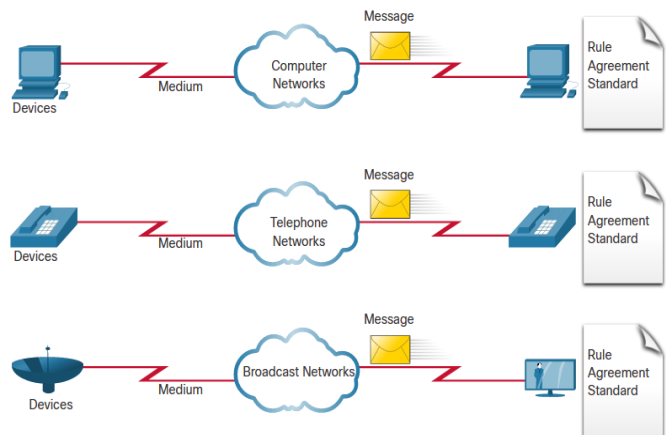


Verbindung	Beschreibung
Dedizierte Standleitung	Dabei handelt es sich um reservierte Leitungen innerhalb des Netzwerks vom Dienstanbieter
Ethernet-WAN	Dadurch wird die LAN-Zugangstechnologie bis ins WAN erweitert.
DSL	Business DSL ist in verschiedenen Formaten verfügbar, einschließlich Symmetric Digital Subscriber Lines (SDSL)
Satellit	Auf diese Weise kann eine Verbindung hergestellt werden, wenn keine kabelgebundene Lösung verfügbar ist.

Konvergentes Netzwerk

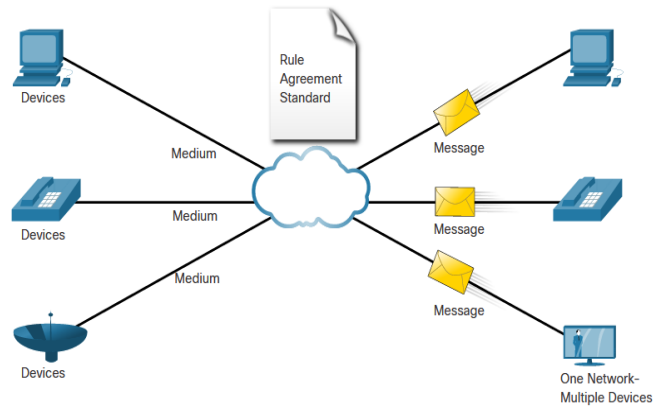
Vor konvergenten Netzwerken war ein Unternehmen für Telefon, Video und Daten separat verkabelt.

- Jedes dieser Netzwerke würde unterschiedliche Technologien verwenden, um das Signal zu übertragen.
- Jede dieser Technologien würde unterschiedliche Regeln und Standards verwenden.



Konvergentes Netzwerk

- Konvergente Datennetze übertragen mehrere Dienste basierend auf einer Verbindungstechnologie:
 - Daten
 - Sprache
 - Video
- Konvergente Netzwerke können Daten, Sprache und Video über dieselbe Netzwerkinfrastruktur bereitstellen. Die Netzwerkinfrastruktur verwendet die gleichen Regeln und Standards.

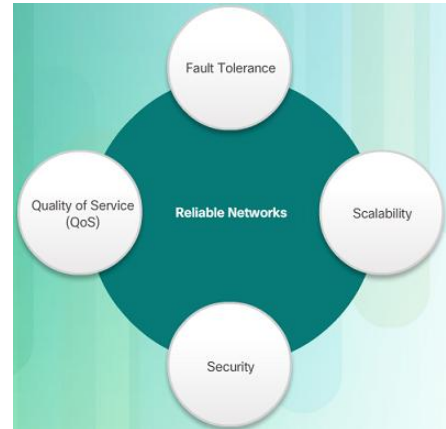


04

Zuverlässige Netzwerke

Netzwerkarchitektur

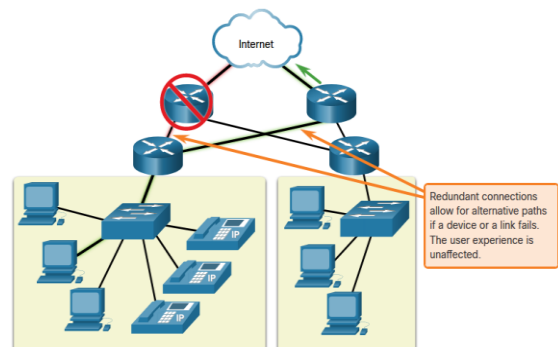
- Der Begriff Netzwerkarchitektur bezieht sich in diesem Zusammenhang auf die Technologien, die die Infrastruktur unterstützen, sowie auf die programmierten Dienste und Regeln oder Protokolle, die Daten über das Netzwerk übertragen.
- Es gibt vier grundlegende Merkmale, die die zugrunde liegenden Architekturen berücksichtigen müssen, um die Erwartungen der Benutzer zu erfüllen:
 - Fehlertoleranz
 - Skalierbarkeit
 - Servicequalität (QoS)
 - Sicherheit



22

Fehlertoleranz

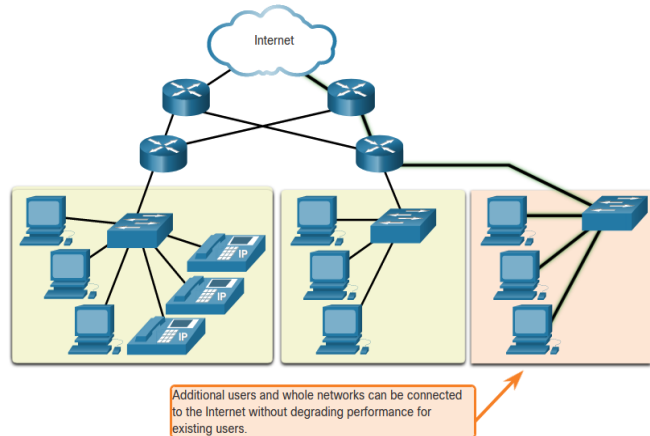
- Ein fehlertolerantes Netzwerk begrenzt die Auswirkungen eines Ausfalls, indem es die Anzahl der betroffenen Geräte begrenzt.
- Für die Fehlertoleranz sind mehrere Pfade erforderlich.
- Paketvermittelnde Netzwerke sind ein Weg, um Redundanz zu bieten:
 - Der Datenverkehr wird in Pakete aufgeteilt, die über ein Netzwerk weitergeleitet werden.
 - Jedes Paket könnte theoretisch einen anderen Weg zum Ziel nehmen.
 - Bei leitungsvermittelten Netzen, die dedizierte Schaltkreise aufbauen, nicht möglich.



23

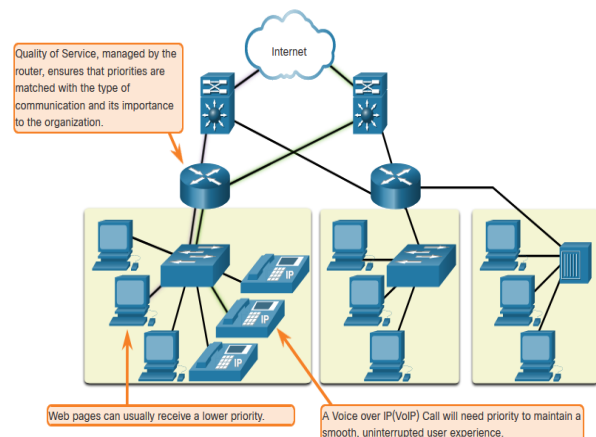
Skalierbarkeit

- Das skalierbare Netzwerk kann schnell und einfach erweitert werden, um neue Benutzer und Anwendungen zu unterstützen, ohne die Leistung der Dienste für bestehende Benutzer zu beeinträchtigen.
- Netzwerkdieser folgen anerkannten Regeln und Protokollen, um die Netzwerke skalierbar zu machen.



Quality of Service

- Sprach- und Live-Videoübertragungen haben höhere Erwartungen an Qualität
- Live-Video mit ständigen Pausen und Pausen erlebt? Dies wird verursacht, wenn eine höhere Nachfrage nach Bandbreite besteht als verfügbar ist – und QoS nicht konfiguriert ist.
- Quality of Service (QoS) ist der primäre Mechanismus, der verwendet wird, um eine zuverlässige Bereitstellung von Inhalten für alle Benutzer zu gewährleisten.
- Mit einer QoS-Richtlinie kann der Router den Fluss von Daten- und Sprachdatenverkehr einfacher verwalten.



Sicherheit

Sicherheit der Netzwerkinfrastruktur

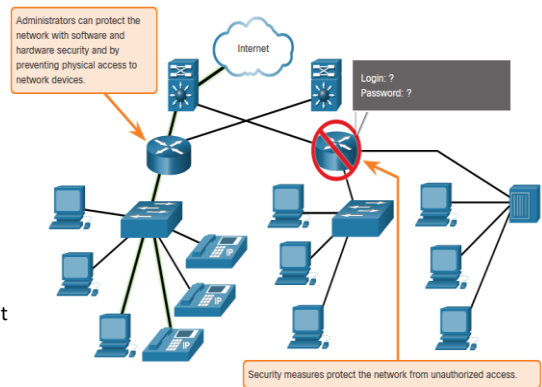
- Physische Sicherheit von Netzwerkgeräten
- Verhinderung von unbefugtem Zugriff auf die Geräte

Informationssicherheit

- Schutz der Informationen oder Daten, die über das Netzwerk übertragen werden

3 Ziele der Netzwerksicherheit:

- **Vertraulichkeit** – nur vorgesehene Empfänger können die Daten lesen
- **Integrität** – Gewissheit, dass die Daten während der Übertragung nicht verändert werden
- **Verfügbarkeit** – Sicherstellung eines zeitnahen und zuverlässigen Zugriffs auf Daten für autorisierte Benutzer

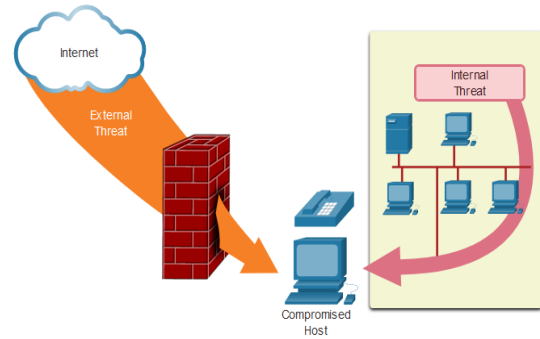


05

Sicherheit

Sicherheitsbedrohungen

- Netzwerksicherheit ist ein integraler Bestandteil des Netzwerks, unabhängig von der Größe des Netzwerks.
- Die implementierte Netzwerksicherheit muss die Umgebung berücksichtigen und gleichzeitig die Daten sichern, aber dennoch die Servicequalität ermöglichen, die vom Netzwerk erwartet wird.
- Die Sicherung eines Netzwerks umfasst viele Protokolle, Technologien, Geräte, Tools und Techniken, um Daten zu sichern und Bedrohungen abzuwehren.
- Bedrohungsvektoren können extern oder intern sein.



Sicherheitsbedrohungen

Externe Bedrohungen

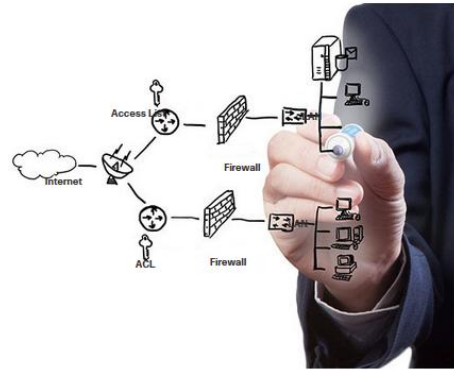
- **Viren, Würmer und Trojaner** - Diese enthalten bösartige Software oder Code, der auf einem Benutzergerät ausgeführt wird.
- **Spyware und Adware** - Diese Arten von Software werden auf dem Gerät eines Benutzers installiert, um heimlich Informationen über den Benutzer zu sammeln.
- **Zero-Day-Angriffe** - Diese Angriffe erfolgen am ersten Tag, an dem eine Schwachstelle bekannt wird.
- **Denial-of-Service-Angriffe** - Diese Angriffe verlangsamen oder stürzen Anwendungen und Prozesse auf einem Netzwerkgerät ab.
- **Abfangen und Diebstahl von Daten** - Bei dieser Art von Angriff werden private Informationen aus dem Netzwerk eines Unternehmens abgefangen.
- **Identitätsdiebstahl** - Bei dieser Art von Angriff werden die Anmeldedaten eines Benutzers gestohlen, um an private Daten zu gelangen.

Interne Bedrohungen

- Verlorene oder gestohlene Geräte
- versehentlicher Missbrauch durch Mitarbeiter
- böswillige Mitarbeiter

Security Solutions

- Sicherheit muss auf mehreren Ebenen mit mehr als einer Sicherheitslösung implementiert werden.
- Netzwerksicherheitskomponenten für Heim- oder kleine Büronetzwerke:
 - Auf den Endgeräten sollte Antiviren- und Antispyware-Software installiert werden.
 - Firewall-Filterung, um unbefugten Zugriff auf das Netzwerk zu blockieren.



Security Solutions

- Größere Netzwerke haben zusätzliche Sicherheitsanforderungen:
 - Dediziertes Firewall-System
 - Zugriffskontrolllisten (ACL)
 - Intrusion Prevention Systeme (IPS)
 - Virtuelle private Netzwerke (VPN)
- Die Untersuchung der Netzwerksicherheit beginnt mit einem klaren Verständnis der zugrunde liegenden Switching- und Routing-Infrastruktur.

